UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/835,164	04/13/2001	Shujin Zhang	CISCO-3840	4870

7590	01/19/2005

David B. Ritchie
Thelen Reid & Priest LLP
P. O. Box 640640
San Jose, CA 95164-0640

EXAMINER
PATEL, NIKETA I

ART UNIT	PAPER NUMBER
2182	

DATE MAILED: 01/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application N .		Applicant(s)	
Offic Action Summary	09/835,164		ZHANG ET AL.	
	Examiner		Art Unit	
	Niketa I. Patel		2182	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE **3** MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *12 November 2004*.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-52* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *29 June 2001* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All b) ☐ Some * c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

<div align="center">

DETAILED ACTION

Claim Rejections - 35 USC § 102

</div>

1.   The following is a quotation of the appropriate paragraphs

of 35 U.S.C. 102 that form the basis for the rejections under

this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) The invention was described in (1) an application for patent, published
> under section 122(b), by·another filed in the United States before the
> invention by the applicant for patent or (2) a patent granted on an
> application for patent by another filed in the United States before the
> invention by the applicant for patent, except that an international
> application filed under the treaty defined in section 351(a) shall have the
> effects for purposes of this subsection of an application filed in the
> United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English
> language.

2.   Claims 1-5, 8-12, 21-26, 29-33, 36-40, 42 and 50-51 are

rejected under 35 U.S.C. 102(e) as being anticipated by Beser

U.S. Patent Number: 6,189,102 (hereinafter referred to as

'*Beser*'.)

3.   **Referring to claims 1, 8, 21, 25, 29, 36, 42, 50, 51,** *Beser*

teaches a method, an apparatus and a programmable storage device

for issuing or renewing a host address, comprising: retrieving a

host identifier in a header of a data packet [see column 32 -

lines 39-67 and column 33 - lines 1-22, 'MAC address']; matching

said host identifier with a list of host identifiers [see column

32 - lines 39-67 and column 33 - lines 1-22, 'test using the

authentication table']; maintaining a state of authentication

for a host if a match is found, or if not matched, maintaining a

state of authentication for a host if a match is found, or if

not matched, maintaining a state of unauthentication for said

host [see column 33 - lines 9-33, 'registered', 'registration

rejected']; inserting a proxy address in a relay agent address

field in the data packet [see column 24 - lines 10-20, 'CM 16

functions as a standard BOOTP relay agent/DHCP Proxy', lines 29-

44 and lines 51-63, 'if the first message field is zero, the

second network device puts its own connection address into the

first message field' and column 26 - lines 36-50]; and

transmitting the data packet to an address allocation device to

issue or renew said host address if said host is in a state of

authentication [see abstract and column 29 - lines 31-48.]

4.   **Referring to claims 2, 9, 22, 30, 37,** *Beser* teaches wherein

said host identifier is a MAC address [see column 32 - lines 39-

67 and column 33 - lines 1-22, 'MAC address'.]

5.   **Referring to claims 3, 10, 31, 38,** *Beser* teaches further

comprising storing said list of host identifiers in a memory

[see column 32 - lines 53-57.]

6.   **Referring to claims 4, 11, 23, 32, 39,** *Beser* teaches

further comprising pairing said list of host identifiers with a

host information list [see column 10 - lines 31-46 and Table 1.]

7.   **Referring to claims 5, 12, 24, 33, 40,** *Beser* teaches

further comprising discarding said data packet if said host is

in a state of unauthentication and wherein said processor is

further adapted to discard said data packet if no match is found

[see column 33 - lines 9-33, 'registration rejected'.]

8.   **Referring to claim 26,** *Beser* teaches wherein said data

packet further comprises a server identifier address field, said

server identifier address field having said proxy address [see

column 18 - lines 8-48.]

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which

forms the basis for all obviousness rejections set forth in this

Office action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at
> the time the invention was made to a person having ordinary skill in the
> art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

10.   Claims 6, 13, 28, 34, 41 are rejected under 35 U.S.C.

103(a) as being unpatentable over Beser U.S. Patent Number:

6,189,102 (hereinafter referred to as 'Beser'.)

11.   **Referring to claims 6, 13, 28, 34, 41,** *Beser* teaches a

method for issuing or renewing a host address [see column 32 -

lines 39-67 and column 33 - lines 1-22, 'MAC address'] however

does not set forth the limitation of further comprising querying

an accounting device to obtain account information for said

host.

It would have been obvious to one of ordinary skill in the

art at the time of applicant's invention that it was old and

well known in the computer art to get the advantage of being

able to obtain account information of a host in order to

determine various types of services that needs to be provided to

the host. It would have been obvious to one or ordinary skill in

the art at the time of applicant's invention to include

accounting device containing account information for the host.

12.   Claims 7, 14-19, 27, 35, 43-49 and 52 are rejected under 35

U.S.C. 103(a) as being unpatentable over Beser U.S. Patent

Number: 6,189,102 (hereinafter referred to as 'Beser') and

further in view of Michael Patrick, "DHCP Relay Agent

Information Option" Motorola ISG, July 30, 1997 (hereinafter

referred to as "Michael".)

13.   **Referring to claims 7, 14, 27, 35, 43,** Beser teaches

inserting a proxy address in a relay agent address field in the

data packet [see column 24 - lines 10-20, 'CM 16 functions as a

standard BOOTP relay agent/DHCP Proxy', lines 29-44 and lines

51-63, 'if the first message field is zero, the second network

device puts its own connection address into the first message

field' and column 26 - lines 36-50] however does not set forth

the limitation of wherein said inserting step further comprises

flagging an option 82 option in said data packet. *Michael*

teaches a use of option 82 with DHCP protocol to prevent several

security attacks on the operation of IP address assignment,

including IP spoofing, Client ID spoofing, MAC address spoofing,

and DHCP server address exhaustion [see *Michael* page 5 -

paragraphs 1,2,3 and page 10 - paragraphs 2,3,4,5,6.]

One of ordinary skill in the art at the time of applicant's

invention would have clearly recognized that it is quite

advantageous for the system of *Beser* to implement option 82 in

order to prevent several security attacks on the operation of IP

address assignment, including IP spoofing, Client ID spoofing,

MAC address spoofing, and DHCP server address exhaustion. It is

for this reason that one of ordinary skill in the art would have

been motivated to use option 82 to prevent various types of

security attacks on the operation of IP address assignment.

14. **Referring to claims 15, 44, 52,** a method and an apparatus

for issuing or renewing a host address, comprising: retrieving a

host identifier in a header of a DHCP request packet [see column

32 - lines 39-67 and column 33 - lines 1-22, 'MAC address'];

matching said host identifier with a list of host identifiers

[see column 32 - lines 39-67 and column 33 - lines 1-22, 'test

using the authentication table']; maintaining a state of

authentication for a host if a match is found, or if not

matched, maintaining a state of unauthentication for said host

[see column 33 - lines 9-33, 'registered', 'registration

rejected']; inserting a proxy address in a relay agent address

field in the data packet [see column 24 - lines 10-20, 'CM 16

functions as a standard BOOTP relay agent/DHCP Proxy', lines 29-

44 and lines 51-63, 'if the first message field is zero, the

second network device puts its own connection address into the

first message field' and column 26 - lines 36-50]; transmitting

the data packet to an address allocation device if said host is

in a state of authentication [see abstract and column 29 - lines

31-48]; setting said proxy address in a server identifier

address field in a DHCP offer packet having an assigned host

address, said DHCP offer packet received from said address

allocation device in response to said DHCP request packet [see

column 18 - lines 8-48]; however does not set forth the

limitation of wherein said inserting step further comprises

flagging an option 82 option in said data packet. *Michael*

teaches a use of option 82 with DHCP protocol to prevent several

security attacks on the operation of IP address assignment,

including IP spoofing, Client ID spoofing, MAC address spoofing,

and DHCP server address exhaustion [see *Michael* page 5 -

paragraphs 1,2,3 and page 10 - paragraphs 2,3,4,5,6.]

One of ordinary skill in the art at the time of applicant's

invention would have clearly recognized that it is quite

advantageous for the system of *Beser* to implement option 82 in

order to prevent several security attacks on the operation of IP

address assignment, including IP spoofing, Client ID spoofing,

MAC address spoofing, and DHCP server address exhaustion. It is

for this reason that one of ordinary skill in the art would have

been motivated to use option 82 to prevent various types of

security attacks on the operation of IP address assignment.

15. **Referring to claims 16, 45,** *Beser* teaches wherein said host

identifier is a MAC address [see column 32 - lines 39-67 and

column 33 - lines 1-22, 'MAC address'.]

16. **Referring to claims 17, 46,** *Beser* teaches further

comprising storing said list of host identifiers in a memory

[see column 32 - lines 53-57.]

17. **Referring to claims 18, 47,** *Beser* teaches further

comprising pairing said list of host identifiers with a host

information list [see column 10 - lines 31-46 and Table 1.]

18. **Referring to claims 19, 48,** *Beser* teaches further

comprising discarding said data packet if said host is in a

state of unauthentication3 [see column 33 - lines 9-33,

'registration rejected'.]

19. **Referring to claims 49,** *Beser* teaches a method for issuing

or renewing a host address [see column 32 - lines 39-67 and

column 33 - lines 1-22, 'MAC address'] however does not set

forth the limitation of further comprising querying an

accounting device to obtain account information for said host.

It would have been obvious to one of ordinary skill in the

art at the time of applicant's invention that it was old and

well known in the computer art to get the advantage of being

able to obtain account information of a host in order to

determine various types of services that needs to be provided to

the host. It would have been obvious to one or ordinary skill in

the art at the time of applicant's invention to include

accounting device containing account information for the host.

Response to Arguments

20. Applicant's arguments filed 11/12/2004 have been fully

considered but they are not persuasive.

The applicant argues that the *Beser* reference does not

disclose (1) matching said host identifier with a list of host

identifiers (2) maintaining a state of authentication for a host

if a match is found, or if not matched, maintaining a state of

unauthentication for said host and (3) transmitting the data

packet to an address allocation device to issue or renew said

host address if said host is in a sate of authentication, at

pages 14, 15, 16, 20, 22 and 24.

The Examiner respectfully disagrees with these arguments.

As per the first argument, *Beser* reference discloses a flow

diagram (FIGS. 21A and 21B FIGS. 21A and 21B) illustrating a

method 384 for authenticating network device in a data-over

cable system for a preferred embodiment of the present

invention. At step 386 of FIG. 21A, a DHCP 66 acknowledgment

message including an IP 54 address for CPE 18 associated CM 16

is received on CMTS 12 during a DHCP 66 initialization sequence

for CPE 18 (FIG. 17). At step 388, a unique identifier is

determined for CPE 18. (e.g., the DHCPOFFER messages (FIG. 17)

have a MAC 44 layer address for CPE 18 in DHCP 6 chaddr-field

132 (FIG. 6), which CMTS 12 stores in one or more routing

tables). **In a preferred embodiment of the present invention, the**

unique identifier (i.e., host identifier) **is a MAC 44 address**

for CPE 18. However, other unique identifiers could also be

used (e.g., a unique Domain Name System identifier). **At step**

390, the IP 54 address and the unique identifier for CPE 18 are

stored in an authentication table on CMTS 12. In a preferred

embodiment of the present invention, the authentication table is

a first Address Resolution Protocol table. However, other

authentication tables could also be used (e.g., a Domain Name

System table). At step 392, the IP 54 address for CPE 18 and a

MAC 44 address for CM 16 are stored in a second Address

Resolution Protocol table on CMTS 12. At step 394, the unique

identifier is optionally added to the DCHP 66 acknowledge

message in DHCP 66 optional-parameter-field 138 (FIG. 6).

However, other DHCP 66 messages could also be used to return the

unique identifier. In another embodiment of the present

invention, the unique identifier is not added to the DCHP 66

acknowledgment message, but is determined from an existing DHCP

66 message field (e.g., a DHCP 66 chaddr-field 132 (FIG. 6) that

contains a MAC 44 address for CPE 18). At step 396, the DHCP 66

acknowledge message is sent to CM 16. At step 398 of FIG. 21B,

a registration message from CM 16 is received on CMTS 12 to

register CPE 18. **The registration messages contains a second**

identifier and a second IP 54 address allegedly for CPE 18, and

a second MAC 44 address allegedly for CM 16. At step 400, a

test is conducted to determine whether the second identifier is

equal to the first unique identifier using the authentication

table on CMTS 12. If the second identifier is equal to the

first unique identifier in the authentication table, then at

step 402, a second test is conducted with a second Address

Resolution Protocol table on CMTS 12 to determine whether the

second IP 54 address allegedly for CPE 18 is equal to the first

IP 54 address for CPE 18, and whether the second MAC 44 address

allegedly for CM 16 is equal to the first MAC 44 address for CM

16. If the network addresses are equal, at step 404 CPE 18 is

registered on CMTS 12. In another embodiment of the present

invention, the second MAC 44 address can also be allegedly for

CMTS 12 or CPE 18 [see column 32, lines 39-67 and column 33,

lines 1-22] i.e., matching said host identifier with a list of

host identifiers (emphasis added.)

As per the second argument, *Beser* reference discloses at

step 398 of FIG. 21B, a registration message from CM 16 is

received on CMTS 12 to register CPE 18. **The registration**

messages contains a second identifier and a second IP 54 address

allegedly for CPE 18, and a second MAC 44 address allegedly for

CM 16. At step 400, a test is conducted to determine whether

the second identifier is equal to the first unique identifier

using the authentication table on CMTS 12. If the second

identifier is equal to the first unique identifier in the

authentication table, then at step 402, a second test is

conducted with a second Address Resolution Protocol table on

CMTS 12 to determine whether the second IP 54 address allegedly

for CPE 18 is equal to the first IP 54 address for CPE 18, and

whether the second MAC 44 address allegedly for CM 16 is equal

to the first MAC 44 address for CM 16. **If the network addresses**

are equal, at step 404 CPE 18 is registered on CMTS 12. In

another embodiment of the present invention, the second MAC 44

address can also be allegedly for CMTS 12 or CPE 18. **If the**

first unique·identifier is not equal to the second identifier at

step 400, registration of CPE 18 is rejected at step 406 [see

column 33, lines 6-25] i.e., maintaining a state of

authentication for a host if a match is found, or if not

matched, maintaining a state of unauthentication for said host

(emphasis added.)

    As per the third argument, *Beser* reference discloses at

FIG. 2, CM 16 includes a Dynamic Host Configuration Protocol

("DHCP") layer 66, hereinafter DHCP 66. DHCP 66 is used to

provide configuration parameters to hosts on a network (e.g., an

IP 54 network). DHCP 66 consists of two components: a protocol

for delivering host-specific configuration parameters from a

DHCP 66 server to a host and **a mechanism for allocation of**

network host addresses to hosts. DHCP 66 is built on a client-

server model, where designated DHCP 66 servers allocate network host addresses and deliver configuration parameters to dynamically configured network host clients.

FIG. 6 is a block diagram illustrating a DHCP 66 message structure 108. The format of DHCP 66 messages is based on the format of BOOTstrap Protocol ("BOOTP") messages described in RFC-951 and RFC-1542 incorporated herein by reference. From a network host client's point of view, DHCP 66 is an extension of the BOOTP mechanism. This behavior allows existing BOOTP clients to interoperate with DHCP 66 servers without requiring any change to network host the clients' BOOTP initialization software. DHCP 66 provides persistent storage of network parameters for network host clients.

To capture BOOTP relay agent behavior described as part of the BOOTP specification and to allow interoperability of existing BOOTP clients with DHCP 66 servers, DHCP 66 uses a BOOTP message format. Using BOOTP relaying agents eliminates the necessity of having a DHCP 66 server on each physical network segment. DHCP 66 message structure 108 includes an operation code field 110 ("op"), a hardware address type field 112 ("htype"), a hardware address length field 114 ("hlen"), a number of hops field 116 ("hops"), a transaction identifier field 118 ("xid"), a seconds elapsed time field 120 ("secs"), a

flags field 122 ("flags"), a client IP address field 124

("ciaddr"), a your IP address field 126 ("yiaddr"), a server IP

address field 128 ("siaddr"), a gateway/relay agent IP address

field 130 ("giaddr"), **a client hardware address field 132**

("chaddr"), an optional server name field 134 ("sname"), a boot

file name 136 ("file") and an optional parameters field 138

("options"). Descriptions for DHCP66 message 108 fields are

shown in Table 4.

TABLE 4

DCHP 66 Parameter	Description
OP 110	Message op code/message type. 1 BOOTREQUEST, 2 = BOOTREPLY.
HTYPE 112	Hardware address type(e.g., `1` = 10 Mps Ethernet).
HLEN 114	Hardware address length (e.g. `6` for 10 Mbps Ethernet).
HOPS 116	Client sets to zero, optionally used by relay-agents when booting via a relay-agent.
XID 118	Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server.
SECS 120	Filled in by client, seconds elapsed since client started trying to boot.
FLAGS 122	Flags including a BROADCAST bit.
CIADDR 124	Client IP address; filled in by client in DHCPREQUEST if verifying previously allocated configuration parameters.
YIADDR 126	`Your`(client) IP address.
SIADDR 128 IP	54 address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK and DHCPNAK by server.
GIADDR 130	Gateway relay agent IP 54 address,

	used in booting via a relay-agent.
CHAODR	**Client hardware address (e.g., MAC 132 layer 44 address).**
SNAME 134	Optional server host name, null terminated string.
FILE 136	Boot file name, terminated by a null string.
OPTIONS 138	Optional parameters.

The DHCP 66 message structure shown in FIG. 6 is used to discover IP 54 and other network host interfaces in data-over-cable system 10. **A network host client (e.g., CM 16) uses DHCP 66 to acquire or verify an IP 54 address and network parameters whenever the network parameters may have changed.** Table 5 illustrates a typical use of the DHCP 66 protocol to discover a network host interface from a network host client.

TABLE 5

1. **A network host client broadcasts a DHCPDISCOVER 66 message on its local physical subnet. The DHCPDISCOVER 66 message may include options that suggest values for a network host interface address. BOOTP relay agents may pass the message on to DHCP 66 servers not on the same physical subnet.**

2. DHCP servers may respond with a DHCPOFFER message that includes an available network address in the `yiaddr` field (and other configuration parameters in DHCP 66 options) from a network host interface. DHCP 66 servers unicasts the DHCPOFFER

message to the network host client (using the DHCP/BOOTP relay

agent if necessary) if possible, or may broadcast the message

to a broadcast address (preferably 255.255.255.255) on the

client's subnet.

3. The network host client receives one or more DHCPOFFER

messages from one or more DHCP 66 servers. The network host

client may choose to wait for multiple responses.

4. The network host client chooses one DHCP 66 server

with an associated network host interface from which to

request configuration parameters, based on the configuration

parameters offered in the DHCPOFFER messages [see column 14,

lines 25-67, column 15, lines 1-67] i.e., transmitting the data

packet to an address allocation device to issue or renew said

host address if said host is in a sate of authentication

(emphasis added.)

Furthermore, as per the applicant's request the following

references are furnished to support the rejection of claims 6,

13, 28, 34, 41 and 49. The U.S. Patents granted to (1) Hejza

(Patent Number: 6,577,628; see column 7, lines 45-62) and (2)

Brezak, Jr. et al. (Patent Number: 6,427,209; see column 5,

lines 4-31 and the abstract) teaches querying an accounting

device to obtain account information for said host.

Conclusion

21. **THIS ACTION IS MADE FINAL**. Applicant is reminded of the
extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action
is set to expire THREE MONTHS from the mailing date of this
action. In the event a first reply is filed within TWO MONTHS
of the mailing date of this final action and the advisory action
is not mailed until after the end of the THREE-MONTH shortened
statutory period, then the shortened statutory period will
expire on the date the advisory action is mailed, and any
extension fee pursuant to 37 CFR 1.136(a) will be calculated
from the mailing date of the advisory action. In no event,
however, will the statutory period for reply expire later than
SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier
communications from the examiner should be directed to Niketa I.
Patel whose telephone number is (571) 272 4156. The examiner
can normally be reached on M-F 8:00 A.M. to 5:00 P.M.

If attempts to reach the examiner by telephone are
unsuccessful, the examiner's supervisor, Jeffrey A. Gaffin can
be reached on (571) 272 4146. The fax phone number for the

organization where this application or proceeding is assigned is

703-872-9306.

Information regarding the status of an application may be

obtained from the Patent Application Information Retrieval

(PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system,

see http://pair-direct.uspto.gov. Should you have questions on

access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

NP
01/12/2005
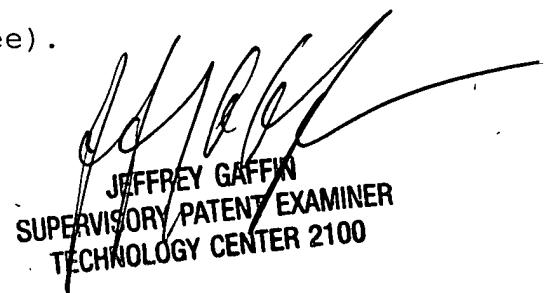
JEFFREY GAFFIN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100